Amendments to the Claims:

The text of all pending claims, (including withdrawn claims) is set forth below. Canceled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (canceled), (withdrawn), (new), (previously presented), or (not entered).

Applicants reserve the right to pursue any canceled claims at a later date.

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1.-23. (canceled)

24. (currently amended) A method for transmitting data, comprising:

by a first user of a communication network:

~~inputting~~ receiving a ~~first data~~first random value originating from a first stochastic process~~ into at least first and second users of a communication network~~;

generating ~~in each of the at least first and second users first and second~~a first symmetrical encryption ~~keys~~ key based on the~~ first data~~ first random value;

transmitting the first random value to a second user of the communication network;

by the second user:

receiving the first random value from the first user; and

generating the first symmetrical encryption key based on the received random value

~~storing the first and second symmetrical encryption keys in each of the at least first and second users for transmitting encrypted data between the at least first and second users; and~~

~~transmitting the encrypted data between the at least first and second users, wherein the encrypted data are generated by changing between the first and second symmetrical encryption keys in a chronological sequence and applying the first respectively second symmetrical encryption key to data to be transmitted.~~

25. (currently amended) The method as claimed in claim 24, wherein the first random value is an input to a function and an output of the function is used to generate the first symmetrical encryption key~~generating the first and second symmetrical encryption keys includes generating a plurality of first data by applying a plurality of combinatorial operations to data originating from the stochastic process~~.

26. (canceled)

27. (currently amended) The method as claimed in claim 24, wherein the first random value is ~~data are~~ obtained by acquiring at least one measured value from the first stochastic process.

28. (previously presented) The method as claimed in claim 24, wherein the first stochastic process includes a time-variable parameter of an automation system.

29. (currently amended) The method as claimed in claim 24,

wherein the first random value is a ~~data are obtained from a Least Significant Bit position related to at least one~~ measured value,

wherein the first user generates the first symmetrical encryption key based on the least significant bits of the first random value in order to at least reduce periodic components of the measured value, and

wherein the second user generates the first symmetrical encryption key based on the least significant bits of the received random value in order to at least reduce periodic components of the measured value.

30. (currently amended) The method as claimed in claim 24, further comprising:

by the second user:

receiving a second random value originating from a second stochastic process;

generating a second symmetrical encryption key based on the second random value;

transmitting the second random value tothe first user;

by the first user:

receiving the second random value from the second user; and

generating the second symmetrical encryption key based on the received random value

~~wherein each of the at least first and second users acquires data originating from the stochastic process for generating the first data~~.

31. (canceled)

32. (canceled)

33. (currently amended) The method as claimed in claim ~~24~~30, wherein the first and second symmetrical encryption keys are generated upon a request by a master user of the communication network.

34. (currently amended) The method as claimed in claim ~~24~~30, wherein the first and second symmetrical encryption keys are generated at predetermined times or after a lapse of a predetermined time interval.

35. (currently amended) The method as claimed in claim ~~26~~24, wherein the first ~~data are~~random value is transmitted over the communication network at a time of low utilization of the communication network.

36. (canceled)

37. (currently amended) The method as claimed in claim 26, wherein the first ~~data are~~random value is transmitted using an asymmetrical encryption method.

38. (canceled)

39. (canceled)

40. (currently amended) A communication system, comprising:

at least first and second users; and

a communication network for transmitting data between the at least first and second users,~~:~~

the first user comprising:

~~an input mechanism for inputting~~a first receiver for receiving a first random value~~data~~ originating from a stochastic process~~ into the at least first and second users of a communication network;~~,

an encryption key generator for generating ~~in each of the at least first and second users first and second~~a first symmetrical encryption ~~keys~~ key based on the first random value~~data; and~~,

a storage unit for storing the first ~~and second~~ symmetrical encryption ~~keys~~ key, and

a transmitter for transmitting the first random value to the second user via the network;

the second user comprising:

a first receiver for receiving the first random value from the first user, and

an encryption key generator for generating the first symmetrical encryption key based on the first random value received from the first user,

~~in each of the at least first and second users for enabling transmission of encrypted data between the at least first and second users, wherein the encrypted data are~~

~~transmitted between the at least first and second users, and the encrypted data are generated by changing between the first and second symmetrical encryption keys in a chronological sequence and applying the first respectively second symmetrical encryption key to data to be transmitted~~

wherein data transferred between the users is encrypted and unencrypted via the first symmetrical encryption key .

41. (previously presented) The communication system as claimed in claim 40, wherein the communication network is a public network.

42. (currently amended) The communication system as claimed in claim 40, wherein the second user further comprises:

a second receiver for receiving a second random value originating from a stochastic process, and

a transmitter for transmitting the second random value to the first user via the network,

the encryption key generator generates a second symmetrical encryption key based on the second random value, and

the storage unit stores the first and the second symmetrical encryption keys,

wherein the first user further comprises:

a second receiver for receiving the secod random value from the second user,

the encryption key generator generates a second symmetrical encryption key based on the second random value, and the storage unit stores the first and the second symmetrical encryption keys,

wherein data transferred between the users is encrypted and unencrypted via the symmetrical encryption keys

~~communication network is the internet, and the first or second user is a master user for triggering the generating of the first and second symmetrical encryption keys by issuing a request via the internet~~.

43. (currently amended) The communication system as claimed in claim ~~40~~42, ~~wherein the communication network is an Ethernet.~~wherein the communication network is the internet, and the first user is a master user for triggering the generating of the first and second symmetrical encryption keys by issuing a request via the internet.

44. (currently amended) The communication system as claimed in claim ~~43~~42, wherein the first or second user is a master user configured to output a command onto the Ethernet for triggering the generation of the first and second symmetrical encryption keys.

45. (new) The method as claimed in claim 24, wherein the first random value is transmitted to a plurality of users and the first symmetrical encryption key is generated at each of the plurality of users.

46. (new) The method as claimed in claim 30, wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to encrypt data transmitted during a second time interval.

47. (new) A method for transmitting data, comprising:

by a first user of a communication network:

storing a first random measured value received from a first stochastic process;

generating a first symmetrical encryption key based on the first random measured value;

transmitting the first measured random value to a second user of the communication network;

receiving the second random measured value from the second user;

generating a second symmetrical encryption key based on the received random value.

by the second user:

storing the second random measured value received from a second stochastic process;

generating the second symmetrical encryption key based on the second random measured value;

transmitting the second measured random value to the first user;

receiving the first random measured value from the first user;

generating the first symmetrical encryption key based on the received measured random value,

wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to encrypt data transmitted during a second time interval.

48. (new) The method as claimed in claim 47, wherein the first random value is an input to a function and an output of the function is used to generate the first symmetrical encryption key.

49. (new) The method as claimed in claim 47, wherein the second random value is an input to a function and an output of the function is used to generate the second symmetrical encryption key.